



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/565,567	01/23/2006	Jorge Abellan Sevilla	09669/081001	2117
22511 7590 08/05/2009 OSHA LIANG L.L.P. TWO HOUSTON CENTER 909 FANNIN, SUITE 3500 HOUSTON, TX 77010				
EXAMINER KANAAN, SIMON P				
ART UNIT 2432		PAPER NUMBER		
NOTIFICATION DATE 08/05/2009		DELIVERY MODE ELECTRONIC		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com

buta@oshaliang.com

### Office Action Summary

**Application No.**

10/565,567

**Applicant(s)**

SEVILLA, JORGE ABELLAN

**Examiner**

SIMON KANAAN

**Art Unit**

2432

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 4/28/2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) \_\_\_\_\_ is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/55/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

#### **DETAILED ACTION**

1. This office action is in response to applicant's amendment filed on **4/28/2009** for Application No. **10/565567**.
2. Applicant's arguments/ amendments with respect to pending claims **1** through **12** filed **4/28/2009**, have been fully considered but they are not persuasive.

#### **Response to Arguments**

3. Applicants amendments are accepted and overcome the prior claim objections, 35 U.S.C. 101 rejections, and 35 U.S.C. 112 second paragraph rejections.
4. Applicant's arguments follow:
  - a. Counter does not count the number of times the data is decrypted
  - b. prior art does not teach "service fee"
  - c. "smart card" is in a different embodiment of the invention in the prior art

In response to Applicant's argumenst:

- a. The limitation "a count of occurrences of decryption steps" does not state "counting the number of times data is decrypted" as Applicant has stated in the arguments. Counting the number of times a key is sent for decryption is a counter for one of the steps of decryption.

In response to Applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., counting the number of decryptions) are not recited in the

rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

- b. Applicant is arguing a newly added limitation and is moot due to new grounds of rejection (see below).
- c. Applicant's argument is not persuasive, in the first embodiment of Andreaux on page 5 lines 17 through 22. The data is stored in memory and is encrypted. i.e. is tamper resistant. The first embodiment does not specifically state a "smart card" however the applicant has amended the claim to specify smart card and not tamper resistant as originally stated.

**Claim Rejections - 35 USC § 103**

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1,2,6, 9, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andreaux et al. (WO 02/47365 A2) in view of Ginter et al. (US PG Publication # 2002/0048369 A1)

As per claims 1 and 9, Andreaux discloses: Method and device for monitoring the usage of a service by a communication device coupled to a smart card,said service

being transmitted from a resource able to communicate with said communication device by way of a network, - Andreaux, page 1, lines 7 and 8, the digital data is transferred in a digital network

said service comprising a plurality of encrypted data flow, the use of said service comprising successive decryption steps of data flow by a respective first key, said first key being encrypted in the data flow – Andreaux, page 8, lines 12 through 20, the information is decrypted multiple times

and decrypted in the smart card by way of a second key stored in said smart card or derived inside said smart card, - Andreaux, page 5, lines 33 through 36, a second key is used for encryption and decryption, and page 8, lines 12 through 20, the smart card stores cryptographic keys)

characterized in that said method comprises the following steps: a. A counting step, in which a memory location stores a count of occurrences of decryption steps of said first key attached to a same service; - Andreaux, page 8, lines 12 through 20, the counter is decremented each time the key is used

but does not specifically disclose the use of a smartcard in the first embodiment of the invention.

However, Andreaux discloses a smart card in the second embodiment. (*page 9, lines 17 through 21, smart card used*)

It would have been obvious for one skilled in the art at the time of the invention to store the data in memory as stated in the first embodiment of Andreaux storing data on

a smart card as stated in the second embodiment of Andreaux because a smart card is a well known form for storing data.

But does not disclose a using step, in which said counter is used to determine a service fee for use of said service

However, Ginter discloses a using step, in which said counter is used to determine a service fee for use of said service –Ginter, [2376] and [1070]

It would have been obvious for one skilled in the art to modify the counter determining device usage in Andreaux with the counter determining device usage which determines tampering in Ginter since determining tampering prevents misuse of product. – Ginter, [1070].

As per claim 2, Andreaux in view of Ginter discloses: Method according to claim 1, characterized in that the smart card stores a predetermined fixed number, and in that it comprises a comparison step in which the incrementing counter is compared to the predetermined fixed number for checking if the counter has reached or not the value of the fixed number; if yes, adequate action can be performed.- Andreaux, page. 8, lines 12-20, counter is decremented, which is incrementing by -1, and compared to zero which is the predetermined fixed number. Action is performed until the counter equals zero

As per claim 6, Andreaux in view of Ginter discloses: Method according to claim 2, characterized in that the action is the completion of decryption steps. –Andreaux, the

data is encrypted and is transmitted a certain number of times with the key if the key is not equal to zero. This is part of the decryption steps.

As per claim 10, Andreaux in view of Ginter discloses: Computer program, stored on a smart card, including program code instructions to execute the counting step of the method defined in claim 1, when said program is executed on the smart card – See rejection to claim 1 above.

7. Claims 3, 5, 7 and 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Andreaux et al. (WO 02/47365 A2) in view of Ginter and in further view of Maillard et al. (US 2002/0048367 A1).

As per claim 3, Andreaux in view of Ginter discloses: Method according to claim 1,

but fails to disclose expressly characterized in that a command is sent to the smart card for renewing the second key.

Maillard discloses characterized in that a command is sent to the smart card for renewing the second key. Maillard, page 4, paragraphs 58 and 59, describes a method including a command sent to the tamper resistant module for the renewing of the key

Andreaux and Maillard are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of sending a command to the tamper resistant module for renewing the key as described by Maillard with the method of monitoring the usage of service as taught by Andreaux because it would prevent the data from being reproduced- Maillard, page 1, paragraph 9, lines 4 and 5.

As per claim 5, Andreaux in view Ginter discloses: Method according to claim 3, but fails to disclose explicitly characterized in that said command is encrypted by a third key known by the smart card.

However, Maillard discloses characterized in that said command is encrypted by a third key known by the smart card. - Maillard, page 4, paragraphs 58 and 59, additional key stored on smart card.

Andreaux and Maillard are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of sending a command to the tamper resistant module for renewing the key as described by Maillard with the method of monitoring the usage of service as taught by Andreaux because it would prevent the data from being reproduced- Maillard, page 1, paragraph 9, lines 4 and 5.

As per claim 7, Andreaux in view of Ginter discloses: Method according to claim 1,



but fails to disclose expressly "characterized in that, each first key is sent periodically, and in that the amount of data is converted into time of use limiting the use of a service in time.

Maillard discloses characterized in that, each first key is sent periodically, - Maillard, page 4, paragraph 58, lines 4 through 7, the encryption key changed monthly hence periodically

and in that the amount of data is converted into time of use limiting the use of a service in time. - Maillard, page 1, paragraph 11, the key is updated periodically according to the subscription. When user terminates subscription they would not retrieve the new key in order to continue decrypting data. Hence the service is limited to time of subscription.

Andreaux and Maillard are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of sending a command to the tamper resistant module for renewing the encryption key periodically as described by Maillard with the method of monitoring the usage of service as taught by Andreaux because it would prevent the data from being reproduced -Maillard, page 1, paragraph 9, lines 4 and 5 and it would allow for subscriptions to a data access service - Maillard, page 1, paragraph 11.

As per claim 12, Andreaux in view of Ginter and in further view of Maillard discloses: Method according to claim 5, characterized in that said commands are transmitted to the smart card by way of the communication device, said communication device including a program for authorizing the transmission of such commands without reading its content – Andreaux, Figure 1, teaches the transmission of data.

8. Claims 4 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andreaux in view of Ginter and in further view of Cutino et al. (EP 1263230 A1).

As per claim 4, Andreaux in view of Ginter discloses: Method according to claim 1,

but fails to disclose expressly “characterized in that a command is sent to the smart card for Resetting/Updating the counter.

Cutino discloses characterized in that a command is sent to the tamper resistant module for Resetting/Updating the counter. - Cutino, column 9, lines 4 through 8, counter is decremented per use, value can be added to card hence updating the counter

Andreaux and Cutino are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of updating the counter as described by Cutino with

the smart card as taught by Andreaux because it is desirable to store monetary value on a card and later replenish it - Cutino, column 9, lines 1 through 8.

As per claim 8, Andreaux in view of Ginter and in further view of Cutino discloses: Method according to claim 4, characterized in that said commands are transmitted to the smart card by way of the communication device, said communication device including a program for authorizing the transmission of such commands without reading its content – Andreaux, Figure 1, teaches the transmission of data.

9. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Andreaux in view of Ginter and in further view of Cutino and in further view of Maillard.

As per claim 11, Andreaux in view of Ginter and in further view of Cutino discloses: Method according to claim 4.

But fails to disclose explicitly characterized in that said command is encrypted by a third key known by the smart card.

However, Maillard discloses characterized in that said command is encrypted by a third key known by the smart card - Maillard, page 4, paragraphs 58 and 59, additional key stored on smart card.

Andreaux and Maillard are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of sending a command to the tamper resistant module for renewing the key as described by Maillard with the method of monitoring the usage of service as taught by Andreaux because it would prevent the data from being reproduced- Maillard, page 1, paragraph 9, lines 4 and 5.

### **Conclusion**

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

11. A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **SIMON KANAAN** whose telephone number is (571)270-3906. The examiner can normally be reached on **Mon-Thurs 7:30-5:00 EST**.

13. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 5712723799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

14. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SIMON KANAAN/  
Examiner, Art Unit 2432

/Gilberto Barron Jr./  
Supervisory Patent Examiner, Art Unit 2432